APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/756,697	01/10/2001	David Stephen Gress	95-456	4607

23164	7590	05/18/2005

LEON R TURKEVICH
2000 M STREET NW
7TH FLOOR
WASHINGTON, DC 200363307

EXAMINER
OSMAN, RAMY M

ART UNIT	PAPER NUMBER
2157	

DATE MAILED: 05/18/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/756,697	GRESS ET AL.
	Examiner	Art Unit	
	Ramy M. Osman	2157	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>25 February 2005</u>.

2a)☒ This action is **FINAL.**   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-78</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-78</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Status of Claims

1.   This communication is responsive to the amendment filed on February 25, 2005. Claims

1-78 are pending. The rejections cited are as stated below.

Claim Rejections - 35 USC § 103

2.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

3.   **Claims 1-5,7-16,18-24,26-33,35-41,43-52,54-62,64-73 and 75-78 rejected under 35**

U.S.C. 103(a) as being unpatentable over Lee et al. (U.S. Patent No. 6,661,877) in view of

Olkin et al. (U.S. Patent No. 6,584,564).

4.   **In reference to claims 1,22,37 and 58, Lee teaches a method, server, computer**

readable medium and a unified communications system comprising:

Receiving from a requesting device a request for providing a user interface session by

the unified communications system to enable a user of the requesting device to send a message

to an identified destination subscriber (column 4 lines 20-45, column 7 lines 45-60, column 8

lines 5-20 & 36-45);

Receiving the message from the requesting device as part of the user interface session (column 5 lines 20-67 and column 8 lines 5-30 & 36-48);

Outputting the message to a determined destination based on determined subscriber profile attributes for the identified destination subscriber (column 8 lines 35-67).

Lee fails to explicitly teach a first prompt. However, Olkin teaches a secure messaging service (Abstract) including: Generating for the requesting device as part of the user interface session a first prompt enabling the user to select encryption of the message (column 6 lines 29-45, column 6 line 61 – column 7 line 10 and column 10 lines 4-16, Olkin discloses a first "send securely" prompt enabling the user to encrypt the email).

It would have been obvious for one of ordinary skill in the art to modify Lee by generating for the requesting device as part of the user interface session a first prompt enabling the user to select encryption of the message, as per the teachings of Olkin for the purpose of making a secure messaging system.

Lee fails to explicitly teach a second prompt. However, Olkin teaches a secure messaging service (Abstract) including: Generating for the requesting device as part of the user interface session a second prompt, based on the user selecting encryption of the message for the user to supply an encryption key (column 4 lines 5-15, column 11 lines 34-67, column 12 lines 44-55 and column 13 lines 53-57, Olkin discloses a second prompt for prompting the user to supply an encryption MessageKey via entering a password. When the user enters a password, a key is generated; and thus a user supplies a key).

It would have been obvious for one of ordinary skill in the art to modify Lee by generating for the requesting device as part of the user interface session a second prompt, based

on the user selecting encryption of the message for the user to supply an encryption key, as per the teachings of Olkin for the purpose of making a secure messaging system.

Lee fails to explicitly teach encrypting the message. However, Olkin teaches a secure messaging service (Abstract) including: Causing encryption of the message into an encrypted message based on the encryption key received from the requesting device as part of the user interface session (column 6 line 61 – column 7 line 10, column 11 lines 55-67 and column 14 lines 1-10, Olkin discloses encrypting the email based on the key).

It would have been obvious for one of ordinary skill in the art to modify Lee by causing encryption of the message into an encrypted message based on the encryption key received from the requesting device as part of the user interface session, as per the teachings of Olkin for the purpose of making a secure messaging system.

Although Lee teaches outputting the message, Lee fails to explicitly teach outputting the encrypted message. However, Olkin teaches a secure messaging service (Abstract) including: Outputting the encrypted message to a determined destination based on determined subscriber profile attributes for the identified destination subscriber (column 3 line 30 – column 4 line 25, column 6 line 61 – column 7 line 10, column 11 lines 55-67 and column 14 lines 1-10).

It would have been obvious for one of ordinary skill in the art to modify Lee by outputting the encrypted message to a determined destination based on determined subscriber profile attributes for the identified destination subscriber, as per the teachings of Olkin for the purpose of making a secure messaging system.

5.   In reference to claims 2,23,38 and 59, Lee in view of Olkin teach claims 1,22,37 and 58

respectively, wherein the causing encryption step includes invoking a prescribed utility for

generation of the encrypted message (Olkin, column 11 lines 55-67 and column 14 lines 1-10).

6.   In reference to claims 3,24,39 and 60, Lee in view of Olkin teach claims 1,23,37 and 58

respectively, wherein the step of receiving the message includes receiving a message data file

having the message and a Multipurpose Internet Mail Extension (MIME) that specifies a format

of the message (Lee, column 6 lines 58-61). Lee fails to explicitly teach the causing encryption

step including encrypting the message data file into an encrypted file having a MIME extension

specifying that the encrypted file has an encrypted format. However, Olkin teaches encrypting

the message data file into an encrypted file having a MIME extension specifying that the

encrypted file has an encrypted format (column 3 lines 30-67 and column 9 lines 40-67).

It would have been obvious for one of ordinary skill in the art to modify Lee by

encrypting the message data file into an encrypted file having a MIME extension specifying that

the encrypted file has an encrypted format, as per the teachings of Olkin for the purpose of

making a secure messaging system.

7.   In reference to claims 4,25,40 and 61, Lee in view of Olkin teach claims 3,22,39 and 60

respectively, generating a message transport header specifying an IP based destination address

corresponding to the identified destination subscriber (Lee, column 8 lines 35-55, inherently

specifies a destination address).

8.   In reference to claim 5,26,41 and 62, Lee in view of Olkin teach claims 3,25,39 and 60

respectively, wherein the message data file has a MIME extension specifying a ".wav" format,

with an audio header and a payload (Lee, column 6 lines 35-60, and column 7 line 55 – column

8 line 30).

9.   In reference to claim 7,43 and 64, Lee in view of Olkin teach claims 1,37 and 58

respectively, wherein the outputting step includes outputting the encrypted message to the

determined destination according to at least one of SMTP protocol and IMAP protocol (Lee,

column 4 lines 7-15 and column 7 lines 20-35).

10.   In reference to claim 8,27,44 and 65, Lee in view of Olkin teach claims 1,37 and 58

respectively, further comprising:

        Receiving from a second requesting device a request for providing a second user

interface session by the unified communications system to enable the identified destination

subscriber using the second requesting device to retrieve stored messages (Lee, column2 lines

54-67, column 7 lines 45-67 and column 8 lines 10-25);

        Retrieving for the second user interface session information related to the stored

messages for the identified destination subscriber (Lee, column 3 lines 1-15 and column 8 lines

10-25).

        Lee fails to explicitly teach encrypted messages. However, Olkin teaches detecting one

of the stored messages as encrypted (column 15 lines 1-15, Olkin discloses identifying a

selected message as encrypted).

        Lee fails to explicitly teach a decryption key. However, Olkin teaches generating for the

second requesting device as part of the second user interface session a third prompt, based on

detecting the one stored message, for the identified destination subscriber to supply a decryption

key (column 15 lines 30-67, Olkin discloses a third prompt for the receiver to supply a

decryption process with a MessageKey, via entering a password).

Lee fails to explicitly teach decrypting the message. However, Olkin teaches supplying

the decryption key and the one stored message to an invoked decryption utility for decryption of

the one stored message into a decrypted data file (column 15 lines 30-67 and column 16 lines

20-55, Olkin discloses decrypting the message based on the key).

It would have been obvious for one of ordinary skill in the art to modify Lee by detecting

one of the stored messages as encrypted; generating for the second requesting device as part of

the second user interface session a third prompt, based on detecting the one stored message, for

the identified destination subscriber to supply a decryption key; and supplying the decryption

key and the one stored message to an invoked decryption utility for decryption of the one stored

message into a decrypted data file, as per the teachings of Olkin for the purpose of making a

secure messaging system.

11.   In reference to claim 9,28,45 and 66, Lee in view of Olkin teach claims 8,44 and 65

respectively, further comprising outputting a decryption result, having been received from the

invoked decryption utility relative to the supplying of the decryption key and one stored

message, during the second user interface session to the identified destination subscriber,

independent of the encryption key matching the decryption key (Olkin, column 16 lines 10-25).

12.   In reference to claim 10,29,46 and 67, Lee in view of Olkin teach claims 1,22,37 and 58

respectively, wherein the receiving step includes receiving the request according to hypertext

transport protocol, each of the steps of generating the first prompt, and generating the second

prompt including sending a corresponding HTML page specifying the corresponding prompt,

the step of receiving the message includes receiving the message as an HTTP post to a

prescribed uniform resource location (Lee, column 4 lines 7-15 and column 7 lines 30-55).

13.   In reference to claims 11,30,47 and 68, Lee teaches a method, server, computer

readable medium and a unified communications system comprising:

receiving from a requesting device a request for providing a user interface session by the

unified communications system to enable a messaging subscriber using the requesting device to

retrieve stored messages (column 2 lines 54-67, column 7 lines 45-67 and column 8 lines 10-

25);

accessing, for the user interface session, subscriber profile information from a subscriber

profile directory according to a prescribed open network protocol (column 3 lines 1-15 and

column 8 lines 10-25).

Lee fails to explicitly teach determining an encrypted message. However, Olkin teaches

a secure messaging service (Abstract) including: determining one of the stored messages is

encrypted based on access of a message store according to a prescribed open network protocol

and based on the accessed subscriber profile information (column 15 lines 1-15 & 30-55, Olkin

discloses identifying a selected message as encrypted).

It would have been obvious for one of ordinary skill in the art to modify Lee by

determining one of the stored messages is encrypted based on access of a message store

according to a prescribed open network protocol and based on the accessed subscriber profile

information, as per the teachings of Olkin for the purpose of making a secure messaging system.

Lee fails to explicitly teach a prompt for a decryption key. However, Olkin teaches a

secure messaging service (Abstract) including: generating for the requesting device as part of

the user interface session a prompt, based on identifying the one stored message as encrypted,

for the messaging subscriber to supply a decryption key (column 15 lines 30-60, Olkin discloses

a prompt for the receiver to supply a decryption process with a MessageKey, via entering a

password).

It would have been obvious for one of ordinary skill in the art to modify Lee by

generating for the requesting device as part of the user interface session a prompt, based on

identifying the one stored message as encrypted, for the messaging subscriber to supply a

decryption key, as per the teachings of Olkin for the purpose of making a secure messaging

system.

Lee fails to explicitly teach decrypting the message. However, Olkin teaches a secure

messaging service (Abstract) including: attempting decrypting of the one stored message based

on the decryption key having been supplied by the messaging subscriber via the requesting

device as part of the user interface session (column 16 lines 10-35, Olkin discloses decrypting

the message based on the key).

It would have been obvious for one of ordinary skill in the art to modify Lee by

attempting decrypting of the one stored message based on the decryption key having been

supplied by the messaging subscriber via the requesting device as part of the user interface

session, as per the teachings of Olkin for the purpose of making a secure messaging system.

14.   In reference to claims 12,31,48 and 69, Lee in view of Olkin teach claims 11,30,47 and

68 respectively, further comprising:

obtaining a decryption result based on the attempting decrypting step; and outputting the

decryption result for attempted presentation to the messaging subscriber (Olkin, column 16 lines

10-60).

15.   In reference to claim 13,32,49 and 70, Lee in view of Olkin teach claims 12,31,48 and 69

respectively, wherein the outputting step includes outputting the decryption result independent

of whether the decryption key enabled successful decryption of the one stored message (Olkin,

column 16 lines 10-25).

16.   In reference to claims 14,35,50 and 71, Lee in view of Olkin teach claims 11,34,47 and

68 respectively, wherein the attempting decrypting step includes invoking a prescribed

decryption utility for generation of the decryption result based on the decryption key (Olkin,

column 16 lines 10-60).

17.   In reference to claims 15,33,51 and 72, Lee in view of Olkin teach claims 11,30,47 and

68 respectively, further comprising obtaining, based on the attempting decrypting step, a

decryption result including a message data file having a message and a Multipurpose Internet

Mail Extension (MIME) that specifies a format of the message (Olkin, column 9 lines 40-67 and

column 15 lines 1-15).

18.   In reference to claim 16,36,52 and 73, Lee in view of Olkin teach claims 11,30,47 and 68

respectively, wherein the receiving step includes receiving the request according to hypertext

transport protocol, wherein the step of generating the prompt includes outputting a first HTML

page specifying the prompt (Lee, column 4 lines 7-15 and column 7 lines 30-55).

19.   In reference to claim 18,54 and 75, Lee in view of Olkin teach claims 17,53 and 74

respectively, wherein the determining step includes:

accessing the message store according to IMAP protocol for messaging information

related to the stored message for the messaging subscriber, based on the accessed subscriber

profile information (Lee, column 4 lines 7-15 and column 7 lines 20-35); and

identifying the one stored message as encrypted based on a prescribed file extension

specifying that the one stored message has an encrypted format (Olkin, column 9 lines 40-67

and column 15 lines 1-40).

20.   In reference to claim 19,55 and 76, Lee in view of Olkin teach claims 18,54 and 75

respectively, wherein the identifying step includes identifying the prescribed file extension as a

MIME type extension that specifies an encrypted format (Lee, column 6 lines 58-61).

21.   In reference to claim 20,56 and 77, Lee in view of Olkin teach claims 11,47 and 68

respectively, wherein the determining step includes:

accessing the message store according to IMAP protocol for messaging information

related to the stored message for the messaging subscriber, based on the accessed subscriber

profile information (Lee, column 4 lines 7-15 and column 7 lines 20-35); and

identifying the one stored message as encrypted based on a prescribed file extension

specifying that the one stored message has an encrypted format (Olkin, column 9 lines 40-67

and column 15 lines 1-40).

22.   In reference to claim 21,57 and 74, Lee in view of Olkin teach claims 20,56 and 77

respectively, wherein the identifying step includes identifying the prescribed file extension as a

MIME type extension that specifies an encrypted format (Lee, column 6 lines 58-61).

23.   Claim 6,17,25,34,42,53,63 and 74 rejected under 35 U.S.C. 103(a) as being

unpatentable over Lee et al. (U.S. Patent No. 6,661,877) in view of Olkin et al. (U.S. Patent

No. 6,584,564) in further view of Edmunds et al. (U.S. Patent No. 6,412,079).

24.   In reference to claims 6,17,42,53,63 and 74, Lee in view of Olkin teach claims

1,11,37,47,58 and 68 respectively. Lee fails to explicitly teach determining the subscriber profile

attributes for the identified destination subscriber based on accessing a subscriber directory

according to Lightweight Directory Access Protocol (LDAP), the subscriber profile attributes

specifying the determined destination. However, Edmunds teaches accessing a directory

according to the well known standard LDAP protocol within a unified messaging system

(Abstract, column 8 lines 30-50 and column 10 lines 3-24).

        It would have been obvious for one of ordinary skill in the art to modify Lee by

determining the recipient of the message by accessing a subscriber directory according to LDAP

protocol for retrieval of destination information as per the teachings of Edmunds because LDAP

is a well known standard facilitating directory searching.

25.   In reference to claims 25 and 34, Lee in view of Olkin teach the above mentioned claims

including the SMTP and IMAP protocols (Lee, column 4 lines 7-15 and column 7 lines 20-35).

Lee fails to explicitly teach accessing a subscriber directory according to Lightweight Directory

Access Protocol (LDAP). However, Edmunds teaches accessing a directory according to the

well known standard LDAP protocol within a unified messaging system (Abstract, column 8

lines 30-50 and column 10 lines 3-24).

        It would have been obvious for one of ordinary skill in the art to modify Lee by

determining the recipient of the message by accessing a subscriber directory according to LDAP

protocol for retrieval of destination information as per the teachings of Edmunds because LDAP

is a well known standard facilitating directory searching.

Response to Amendment

26.   Examiner acknowledges applicants amendment filed 2/25/2005, where applicant

amended the claims. No claims were cancelled or added.

Response to Arguments

27.   Applicant's arguments with respect to claims 1-78 have been considered but are not

persuasive.

28.   In response to applicant's argument that the references fail to show certain features of

applicant's invention, it is noted that the features upon which applicant relies (i.e., server) are not

recited in the rejected claim(s). Although the claims are interpreted in light of the specification,

limitations from the specification are not read into the claims. See *In re Van Geuns*, 988

F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

29.   Applicant argues that Olkin fails to teach the server generating the prompts. However, the

claims do not mention a server, and do not mention a server generating a prompt. Therefore the

claims are broad and are broadly interpreted.

30.   Applicant argues that Olkin fails to teach a user interface session between a server and a

sender or receiver. However, the claims do not mention a server, and do not mention that the

interface session is between a server and a sender or receiver. Therefore the claims are broad and

are broadly interpreted.

31.   Applicant's amendment necessitated the new ground(s) of rejection presented in this

Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a).

Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this

final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Ramy M. Osman whose telephone number is (571) 272-4008.

The examiner can normally be reached on M-F 9-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ario Etienne can be reached on (571) 272-4001. The fax phone number for the

organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

RMO
May 8, 2005

SALEH NAJJAR
PRIMARY EXAMINER